Практическая работа №14
Динамическая маршрутизация

Маршрутизация - процесс определения в сети наилучшего пути, по которому пакет может достигнуть адресата. *Динамическая маршрутизация* может быть осуществлена с использованием одного и более протоколов (*RIP* v2, *OSPF* и др.).

Новый термин

Динамическая маршрутизация — вид маршрутизации, при котором таблица маршрутизации заполняется и обновляется автоматически при помощи одного или нескольких протоколов маршрутизации (RIP, OSPF, EIGRP, BGP).

Каждый *протокол маршрутизации* использует свою систему оценки маршрутов (*метрику*). *Маршрут* к сетям назначения строится на основе таких критериев как

- количество ретрансляционных переходов
- пропускная способность канала связи
- задержки передачи данных
- и др.

Маршрутизаторы обмениваются друг с другом информацией о маршрутах с помощью служебных пакетов по протоколу *UDP*. Такой обмен информации увеличивает наличие дополнительного трафика в сети и нагрузку на эту *сеть*. Возможна также ситуация, при которой таблицы маршрутизации на роутерах не успевают согласоваться между собой, что может повлечь появление ошибочных маршрутов и потерю данных.

Протоколы маршрутизации делятся на три типа:

- Дистанционно векторные протоколы (RIP)
- Протоколы с отслеживанием состояния каналов (OSPF)
- Смешанные протоколы (EIGRP)

И др.

Протокол RIP

RIP — протокол дистанционно-векторной маршрутизации, использующий для нахождения оптимального пути *алгоритм* Беллмана-Форда. *Алгоритм* маршрутизации *RIP* - один из самых простых протоколов маршрутизации. Каждые 30 секунд он передает в *сеть* свою таблицу маршрутизации. Основное отличие протоколов в том, что RIPv2 (в отличие от RIPv1) может работать по мультикасту, то есть, рассылаясь на мультикаст *адрес*. Максимальное количество "хопов" (шагов до места назначения), разрешенное в RIP1, равно 15 (*метрика* 15). Ограничение в 15 хопов не дает применять *RIP* в больших сетях, поэтому протокол наиболее распространен в небольших компьютерных сетях. Вторая версия протокола — протокол RIP2 была разработана в 1994 году и является улучшенной версией первого. В этом протоколе повышена *безопасность* за счет введения дополнительной маршрутной информации. Принцип дистанционно-векторного протокола: каждый *маршрутизатор*, использующий протокол *RIP* периодически широковещательно рассылает своим соседям специальный пакет-*вектор*, содержащий расстояния (измеряются в метрике) от данного маршрутизатора до всех известных ему сетей. *Маршрутизатор* получивший

такой *вектор*, наращивает компоненты вектора на величину расстояния от себя до данного соседа и дополняет *вектор* информацией об известных непосредственно ему самому сетях или сетях, о которых ему сообщили другие маршрутизаторы. Дополненный *вектор маршрутизатор* рассылает всем своим соседям. *Маршрутизатор* выбирает из нескольких альтернативных маршрутов *маршрут* с наименьшим значением метрики, а *маршрутизатор*, передавший информацию о таком маршруте помечается как следующий (*next hop*). Протокол непригоден для работы в больших сетях, так как засоряет *сеть* интенсивным трафиком, а узлы сети оперируют только векторами-расстояний, не имея точной информации о состоянии каналов и топологии сети. Сегодня даже в небольших сетях протокол вытесняется превосходящими его по возможностям протоколами *EIGRP* и *OSPF*.

Практическая работа 14-1. Настройка протокола RIP версии 2 для сети из шести устройств

Наша задача – настроить маршрутизацию на схеме, представленной на рис 14.1

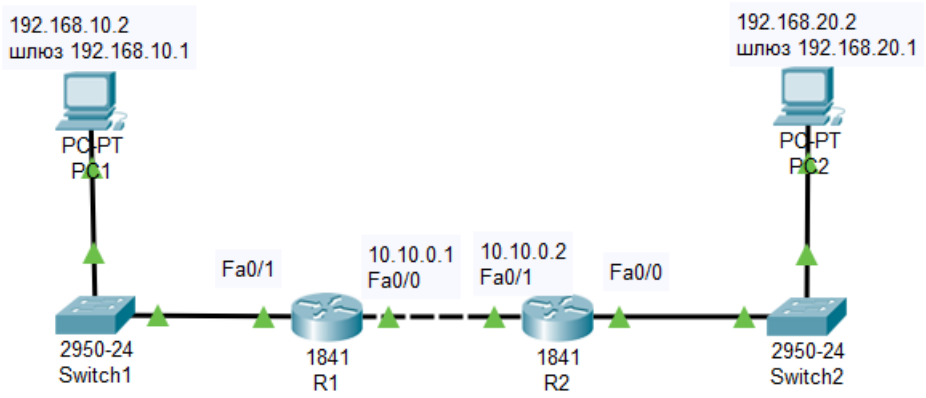


Рис. 14.1. Схема сети

Примечание

При настройке сети не забывайте включать порты.

Настройка протокола RIP на маршрутизаторе R1

Войдите в конфигурации в консоль роутера и выполните следующие настройки (рис 14.2).

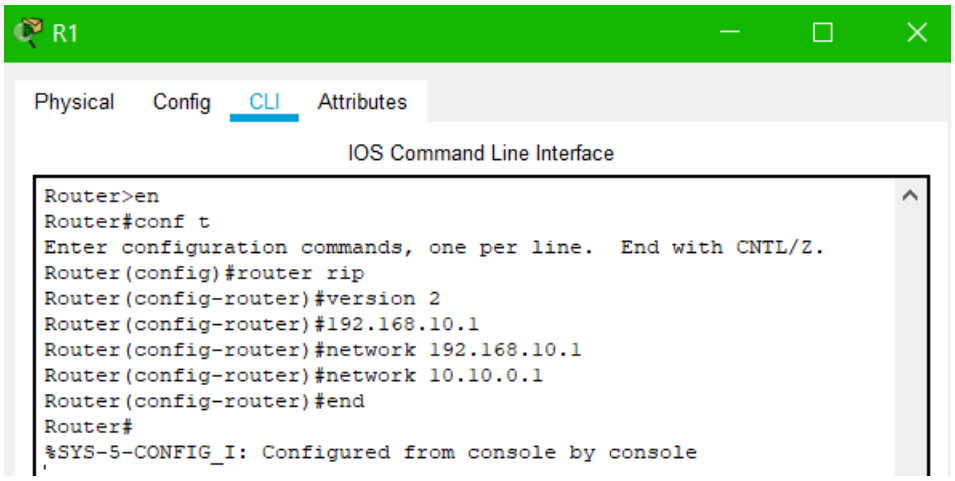


Рис. 14.2. Настройка протокола RIPv2 на маршрутизаторе Router1

Примечание

Router(config)#router rip (Вход в режим конфигурирования протокола RIP).

Router(config-router)#network 192.168.10.1 (Подключение клиентской сети к роутеру со стороны коммутатора S1).

Router(config-router)#network 10.10.0.1 (Подключение второй сети, то есть сети между роутерами).

Router(config-router)#version 2 (Задание использования второй версии протокол RIP).

Настройка протокола RIP на маршрутизаторе R2

Войдите в конфигурации роутера 2 и выполните следующие настройки (рис. 14.3).

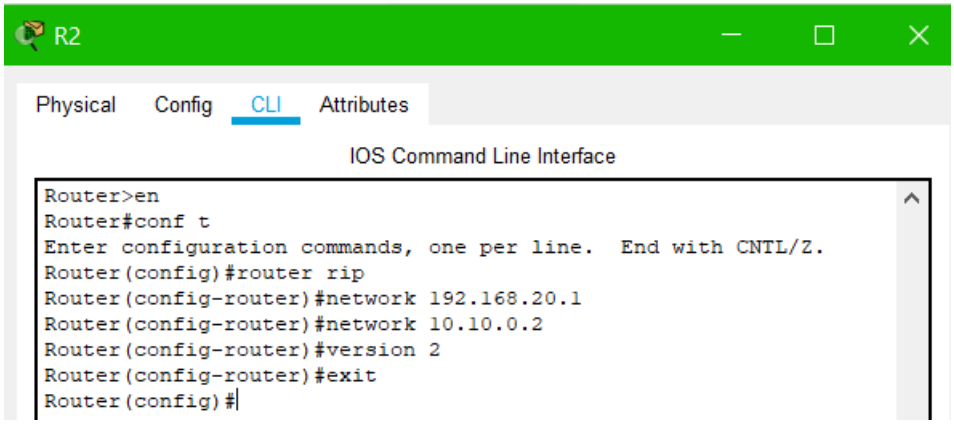


Рис. 14.3. Настройка протокола RIPv2 на маршрутизаторе R2

Проверяем настройки коммутаторов и протокола RIP

Давайте посмотрим настройки протокола RIPv2 на маршрутизаторах R1 и R2 (14.4).

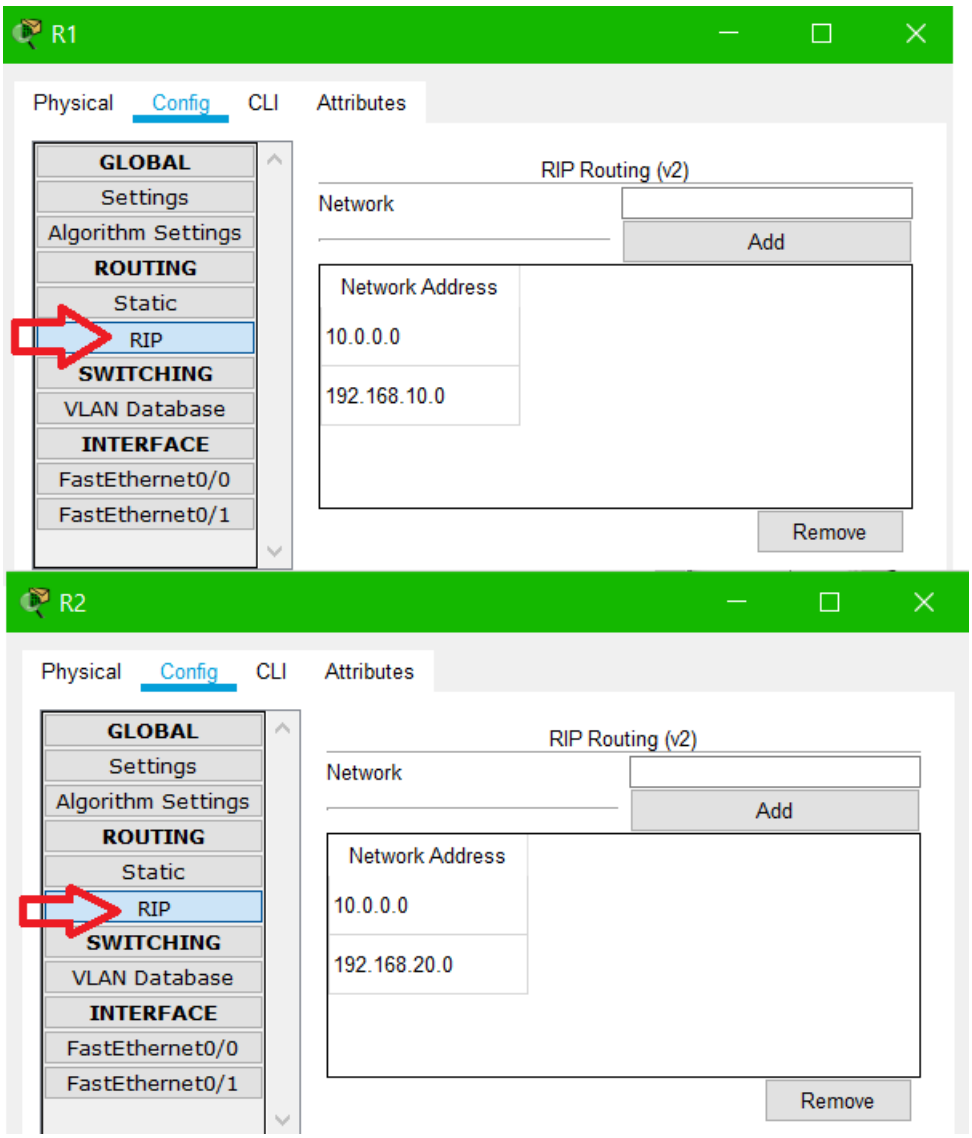


Рис. 14.4. Настройки маршрутизаторов R1 и R2

Чтобы убедиться в том, что маршрутизаторы действительно правильно сконфигурированы и работают корректно, просмотрите таблицу RIP роутеров, используя команду:

Router#show ip route rip (рис 14.5 и 14.6).

```
Router>show ip route rip
R    192.168.10.0/24 [120/1] via 10.10.0.1, 00:00:12, FastEthernet0/1
Router>
```

Рис. 14.5. Таблица маршрутизации R1

Данная таблица показывает, что к сети 192.168.10.0 есть только один маршрут: через R1(сеть 10.10.0.1).

Рис. 14.6. Таблицы маршрутизации R2

Данная таблица показывает, что к сети 192.168.20.0 есть только один маршрут: через R2 (сеть 10.10.0.2).

Проверка связи между PC1 и PC2

Проверим, что маршрутизация производится верно (рис. 5.7).

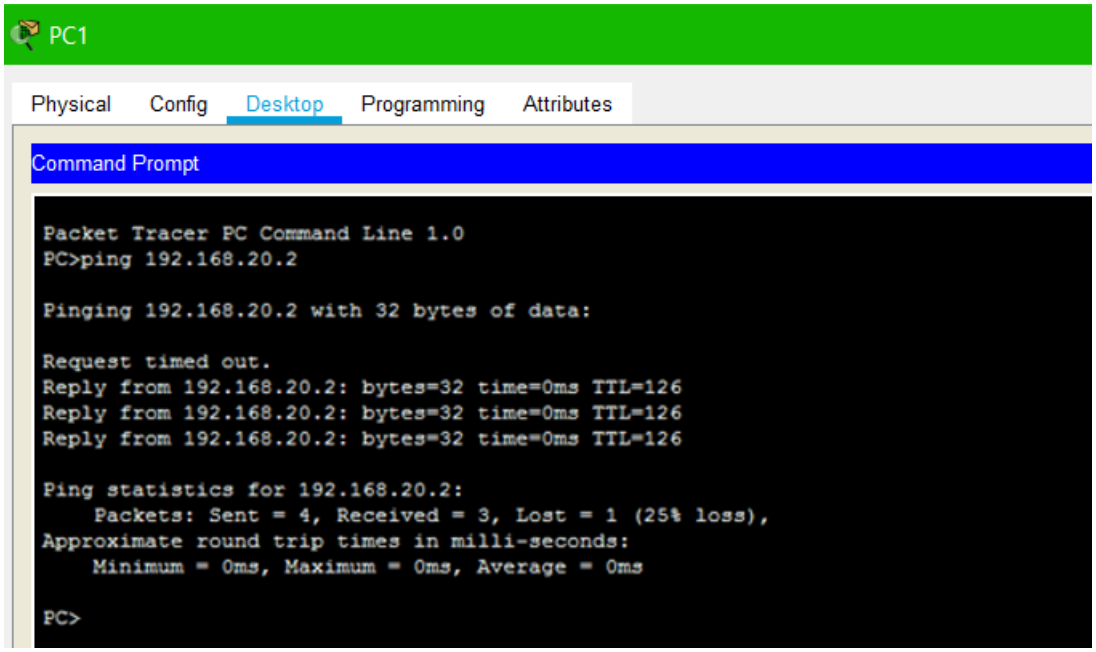


Рис. 5.7. Пинг с PC1 на PC2

Практическая работа 14-2. Конфигурирование протокола RIP версии 2 для сети из четырех устройств

На рис. 14.8. представлена *сеть*, на примере которой мы сконфигурируем *протокол маршрутизации RIP* v2.

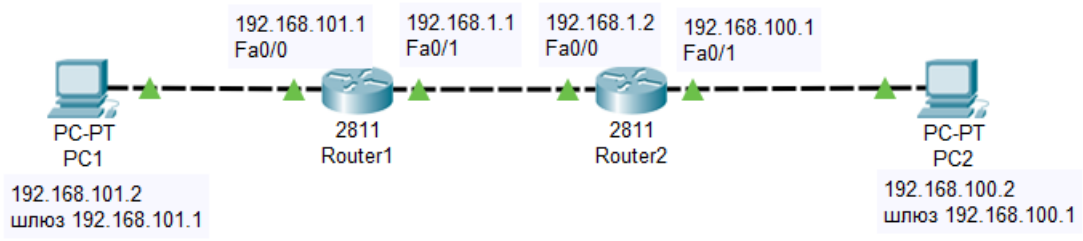


Рис. 14.8. Сеть для конфигурации протоколов маршрутизации

Сначала сконфигурируем R1 (рис. 14.9).

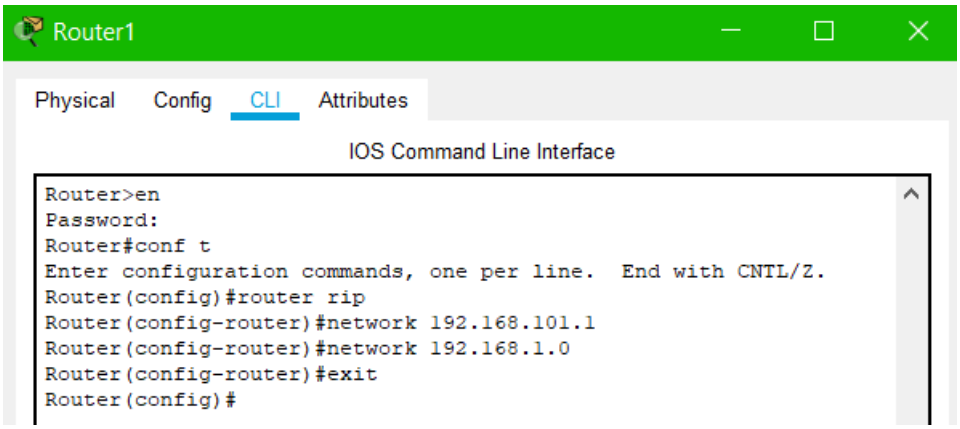


Рис. 14.9. Настройка RIP на R1

Смотрим результат на вкладке **Config** (рис. 14.10).

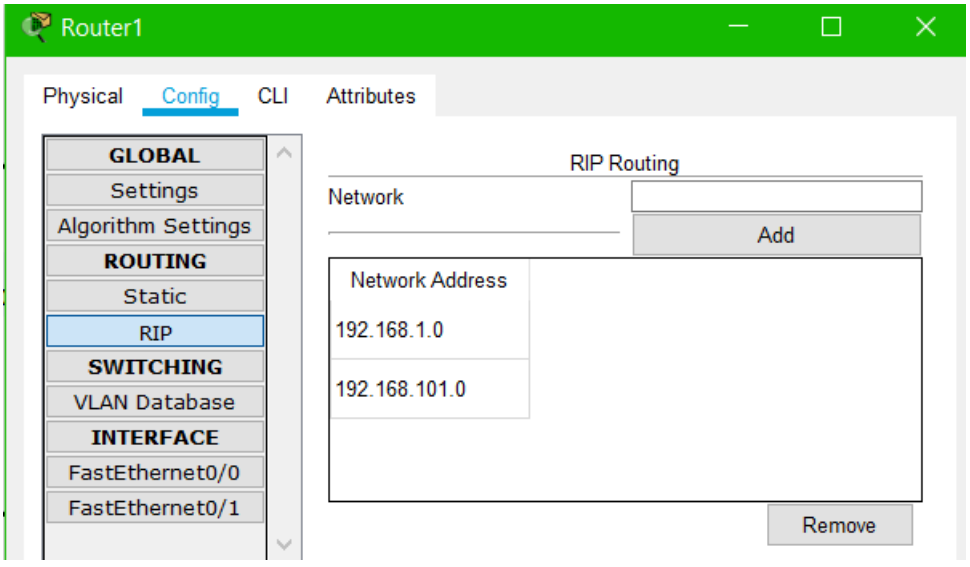


Рис. 14.10. Окно R1,вкладка Config

Конфигурируем R2 (14.11).

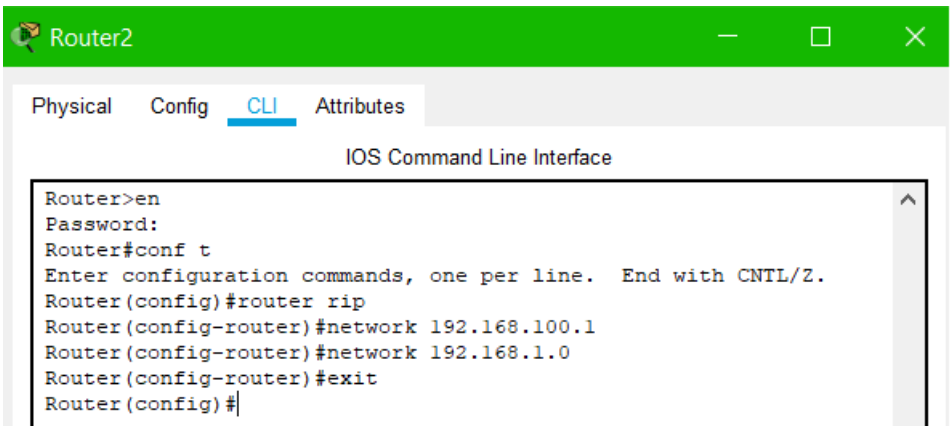


Рис. 14.11. Настройка RIP на R2

Наблюдаем результат (рис. 14.12).

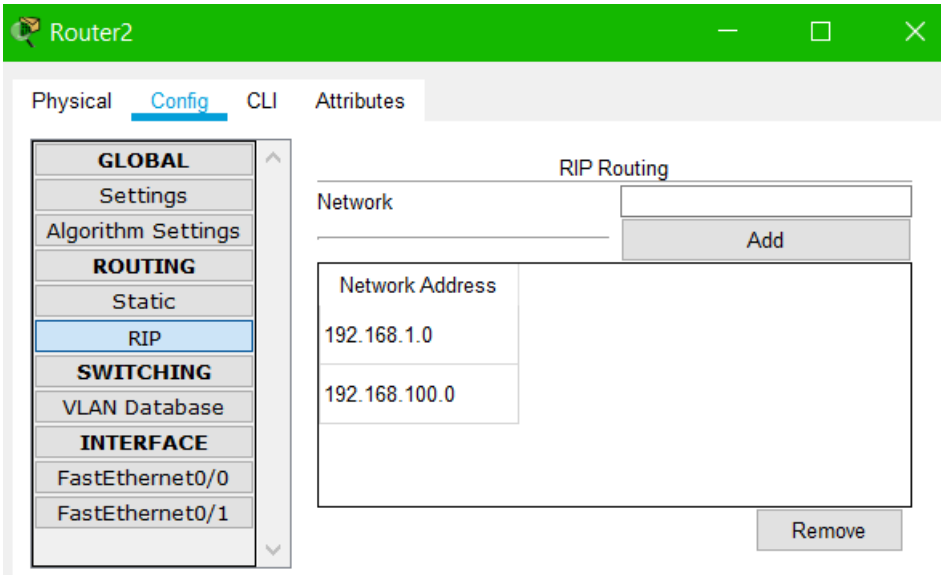


Рис. 14.12. Окно R2, вкладка Config

Проверяем доступность ПК из разных сетей (рис. 14.13_).

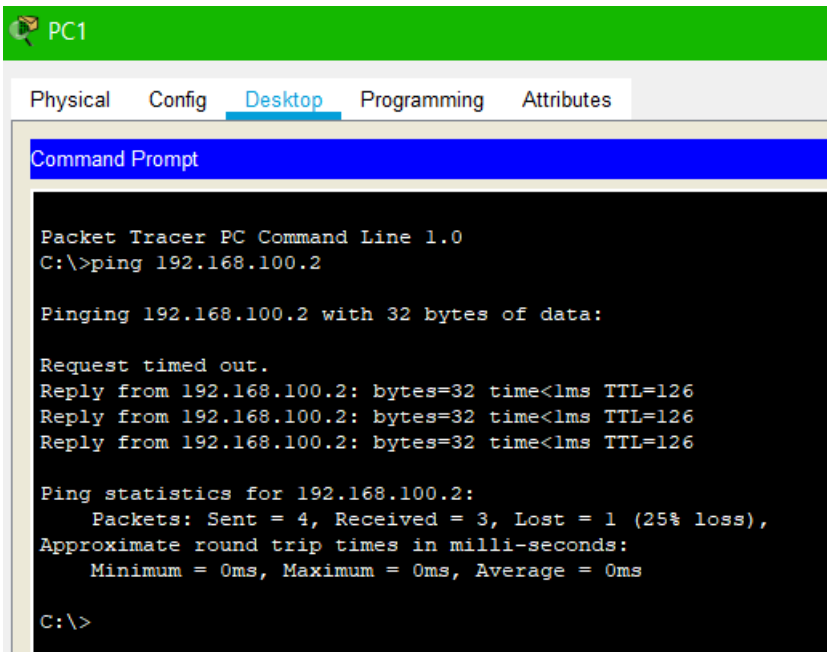


Рис. 14.13. Результат маршрутизации по протоколу RIP

Протокол маршрутизации EIGRP

Протокол *EIGRP* более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем протокол *OSPF*. Также *EIGRP* имеет более продвинутый *алгоритм* вычисления метрики. В формуле вычисления метрики есть возможность учитывать загруженность и *надежность* интерфейсов на пути пакета. Недостатком протокола *EIGRP* является его ограниченность в его использовании только на оборудовании компании Cisco.

Практическая работа 14-3. Конфигурирование протокола EIGRP

Схема сети изображена на рис. 14.14.

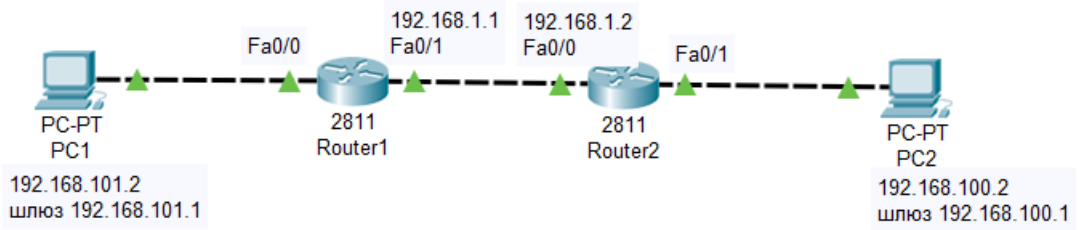


Рис. 14.14. Схема для конфигурации протокола EIGRP

Настройка протокола *EIGRP* очень похожа на настройку протокола *RIP*.

Программирование R1

Конфигурируем R1 (14.15).

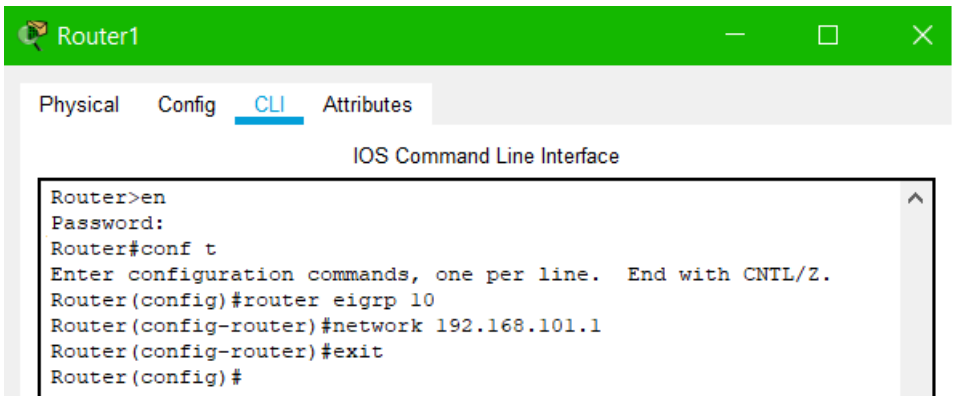


Рис. 5.15. Конфигурирование R1

Программирование R2

Конфигурируем R(рис. 14.16).

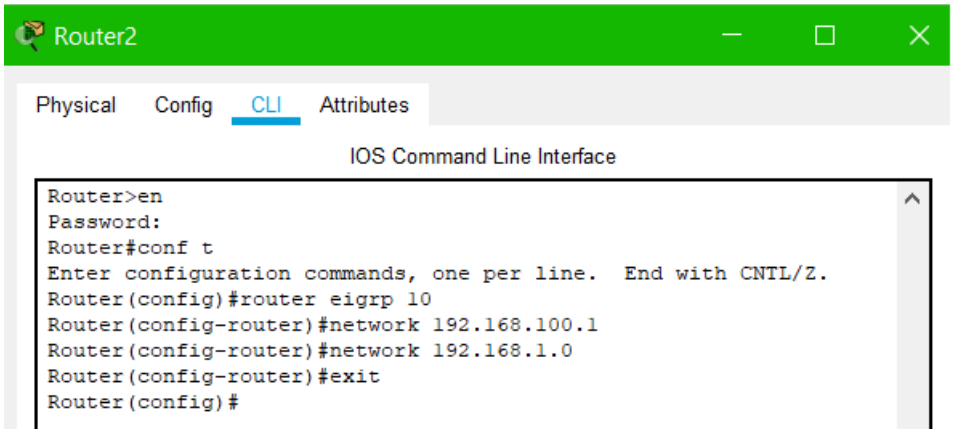


Рис. 14.16. Конфигурирование R2

Проверка работы сети

Проверяем работу маршрутизаторов (рис. 14.17).

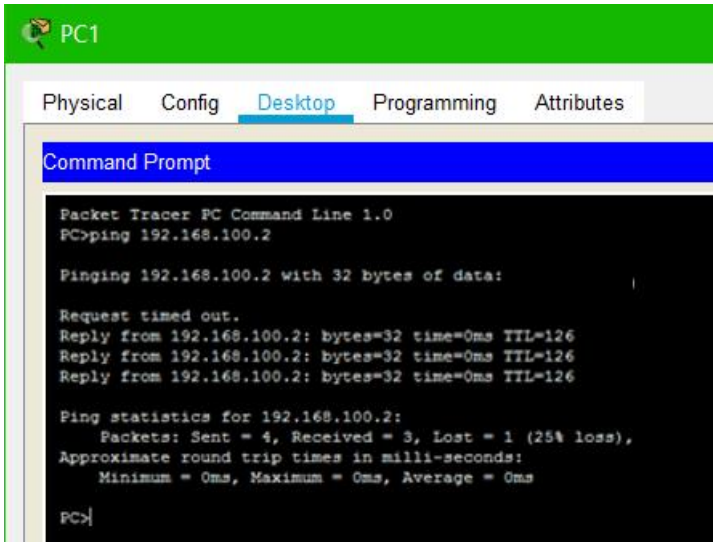


Рис. 14.17. Результат проверки работоспособности сети

Протокол OSPF

Алгоритм работы протокола динамической маршрутизации *OSPF* основан на использовании всеми маршрутизаторами единой *базы данных*, описывающей, с какими сетями связан каждый *маршрутизатор*. Описывая каждую *связь*, маршрутизаторы связывают с ней метрику – *значение*, характеризующее "качество" канала связи. Это позволяет маршрутизаторам *OSPF* (в отличие от *RIP*, где все каналы равнозначны) учитывать реальную пропускную способность канала и выявлять наилучшие маршруты. Важной особенностью протокола *OSPF* является то, что используется групповая, а не широковещательная рассылка (как в *RIP*), то есть, нагрузка каналов меньше.

OSPF (*Open* Shortest *Path First*) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала link-state (*LSA*). Основан на алгоритме для поиска кратчайшего пути. Отслеживание состояния канала требует отправки объявлений о состоянии канала (*LSA*) на активные интерфейсы всех доступных маршрутизаторов зоны. В этих объявлениях содержится описание всех каналов маршрутизатора и *стоимость* каждого канала. *LSA* сообщения отправляются, только если произошли какие-либо изменения в сети, но раз в 30 минут *LSA* сообщения отправляются в принудительном порядке. Протокол реализует *деление* автономной системы на зоны (areas). Использование зон позволяет снизить нагрузку на *сеть* и процессоры маршрутизаторов и уменьшить размер таблиц маршрутизации.

Описание работы протокола:

Все маршрутизаторы обмениваются специальными Hello-пакетами через все интерфейсы, на которых активирован протокол *OSPF*. Таким образом, определяются маршрутизаторы-соседи, разделяющие общий *канал передачи данных*. В дальнейшем hello-пакеты посылаются с интервалом раз в 30 секунд. Маршрутизаторы пытаются перейти в состояние соседства со своими соседями. Переход в данное состояние определяется типом маршрутизаторов и типом сети, по которой происходит обмен hello-пакетами, по зонному признаку. Пара маршрутизаторов в состоянии соседства синхронизирует между собой базу данных состояния каналов. Каждый *маршрутизатор* посылает объявление о состоянии канала своим соседям, а каждый получивший такое объявление записывает информацию в базу данных состояния каналов и рассылает копию объявления другим своим соседям. При рассылке объявлений по зоне, все маршрутизаторы строят идентичную базу данных состояния каналов. Каждый *маршрутизатор* использует *алгоритм SPF* для вычисления графа (дерева кратчайшего пути) без петель. Каждый *маршрутизатор* строит собственную маршрутизацию, основываясь на построенном дереве кратчайшего пути.

Прямая и обратная маска

В оборудовании **Cisco** иногда приходится использовать обратную маску, то есть не привычную нам **255.255.255.0** (Subnet mask — прямая *маска*), а **0.0.0.255** (Wildcard mask — обратная *маска*). Обратная *маска* используется в листах доступа (*access list*) и при описании сетей в протоколе **OSPF**. Прямая *маска* используется во всех остальных случаях. Отличие масок заключается также в том, что прямая *маска* оперирует сетями, а обратная — хостами. С помощью обратной маски вы можете, например, выделить во всех подсетях хосты с конкретным адресом и разрешить им *доступ* в *Интернет*. Так, как чаще всего в локальных сетях используют адреса типа 192.168.1.0 с маской 255.255.255.0, то самая распространенная Wildcard mask (шаблонная *маска* или обратная *маска*, или инверсная *маска*) - *маска* 0.0.0.255.

Новый термин

Шаблонная маска (wildcard mask) — маска, указывающая на количество хостов сети. Является дополнением для маски подсети. Вычисляется по формуле для каждого из октетов маски подсети как 255-маска_подсети. Например, для сети 192.168.1.0 и маской подсети 255.255.255.240 шаблонная маска будет выглядеть как 0.0.0.15. Шаблонная маска используется в настройке некоторых протоколов маршрутизации, а также является удобным параметром ограничений в списках доступа.

Расчёт Wildcard mask

Существует *связь*, между обратной и *прямой* маской: в сумме эти маски по каждому разряду должны составлять 255. Пусть наша *сеть* 192.168.32.0 /28. Рассчитает wildcard mask: *префикс* /28 это 255.255.255.240 или 11111111.11111111.11111111.11110000. Для wildcard mask нам нужны только нули, то есть, 11110000 переводим в десятичное число и считаем: 128/64/32/16/8/4/2/1 это будет 8+4+2+1=15, т.е. наша wildcard mask будет равна 0.0.0.15.

Самостоятельно

Дана прямая *маска* **255.255.255.248**. Выполните расчет и докажите, что обратная равна **0.0.0.7**.

Практическая работа 14-4. Пример конфигурирования протокола OSPF для 4-х устройств

Соберите схему, изображенную на рис. 14.18

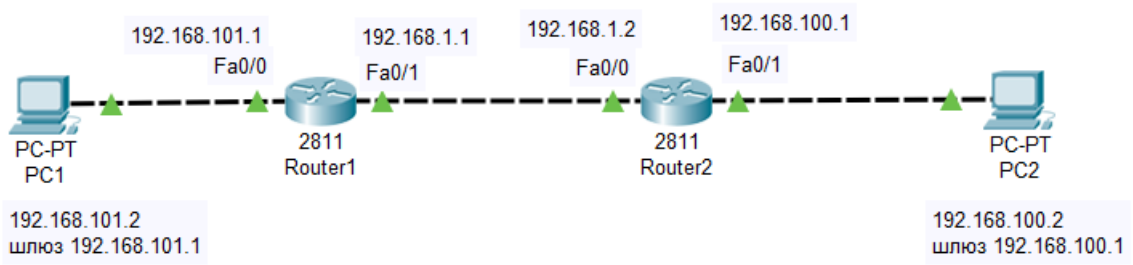


Рис. 14.18 Схема для конфигурации протокола OSPF

Настройка роутеров

Выполним конфигурирование R1 (рис. 14.19).

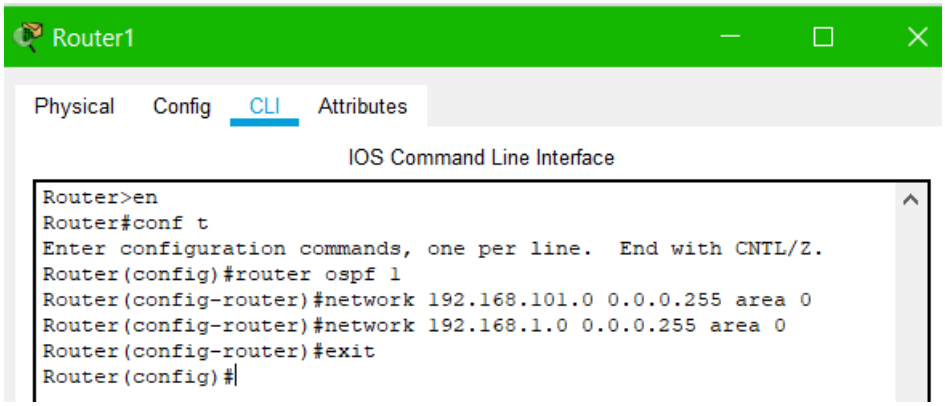


Рис. 14.19. Настройка R1

Теперь выполним настройки R2 (рис. 14.20).

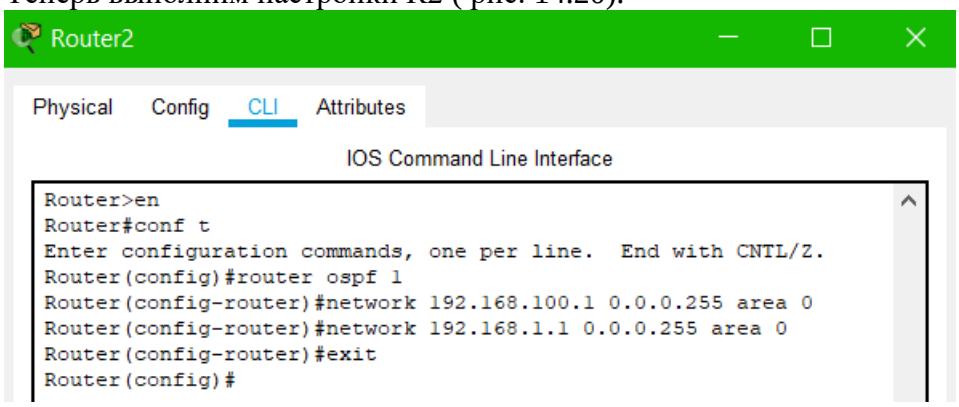


Рис. 14.20. Настройка R2

Совет

Если вам потребуется в CPT сбросить настройки роутера, то следует выключить его тумблер питания, а затем снова включить.

Проверка результата

Для проверки маршрутизации пропингуем ПК из разных сетей (рис. 14.21).

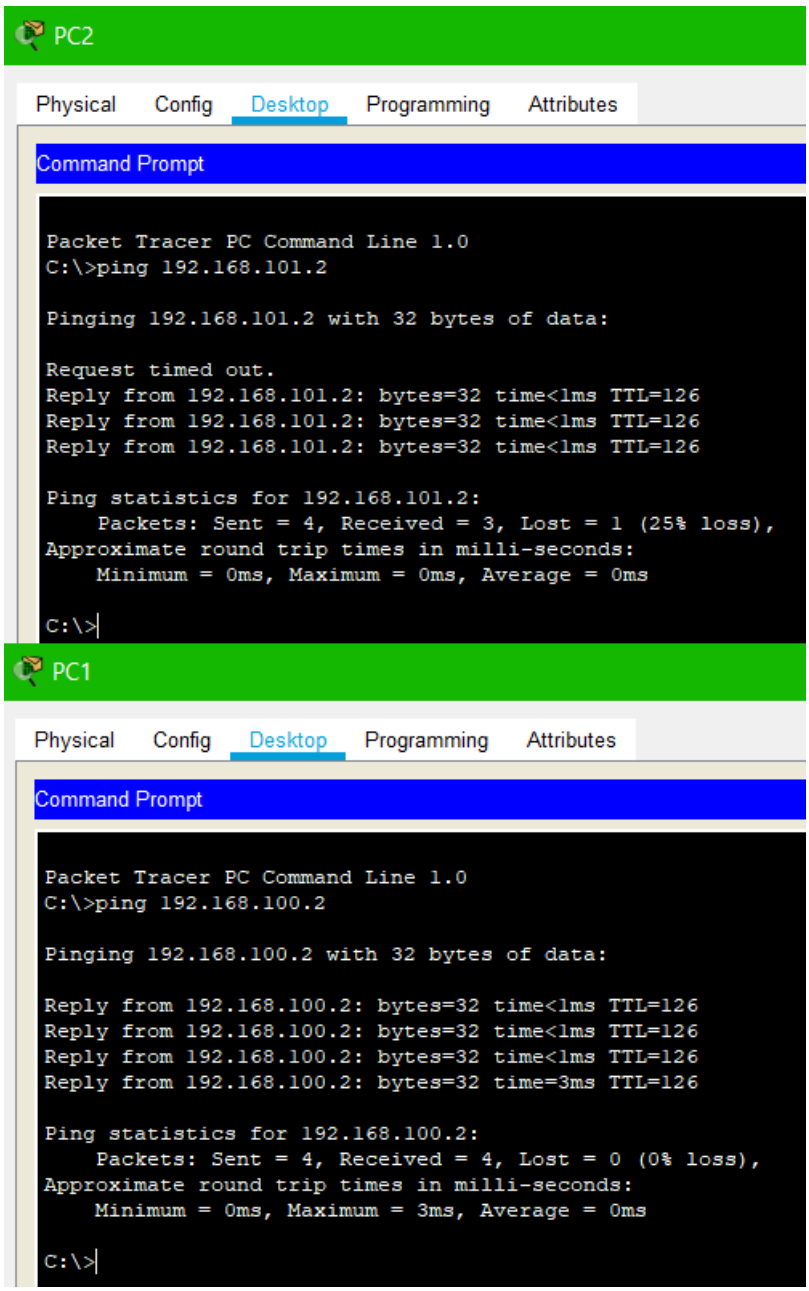


Рис. 14.21. Результат проверки работоспособности OSPF

Практическая работа 14-5. Настройка маршрутизации по протоколу OSPF для 6 устройств

Постройте следующую схему (рис. 14.22).

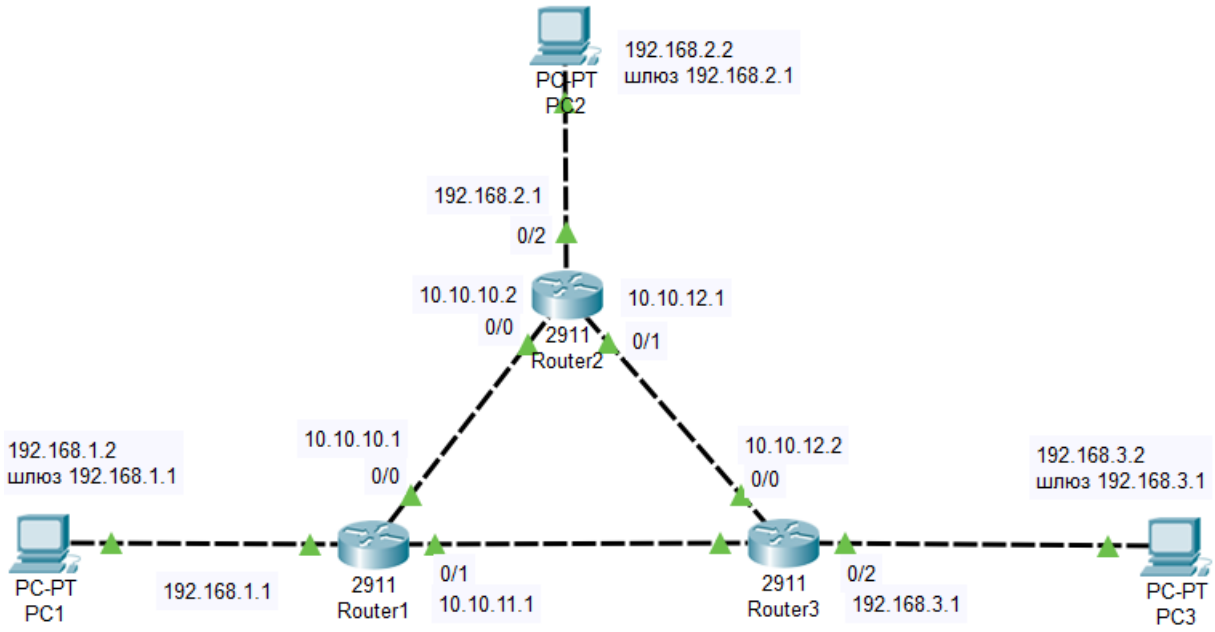


Рис. 14.22. Начальная схема сети для нашей работы

Цель работы – настроить маршрутизацию в данной сети по протоколу *OSPF*.

Настроим loopback интерфейс на R1

На R1 настроим программный **loopback интерфейс** — алгоритм, который направляет полученный сигнал (или данные) обратно отправителю (рис. 14.23).

Примечание
IPv4-адрес, назначенный loopback-интерфейсу, может быть необходим для процессов маршрутизатора, в которых используется IPv4-адрес интерфейса в целях идентификации. Один из таких процессов — алгоритм кратчайшего пути (OSPF). *При включении интерфейса loopback для идентификации маршрутизатор будет использовать всегда доступный адрес интерфейса loopback,* а не IP-адрес, назначенный физическому порту, работа которого может быть нарушена. На маршрутизаторе можно активировать несколько интерфейсов loopback. IPv4-адрес для каждого интерфейса loopback должен быть уникальным и не должен быть задействован другим интерфейсом.

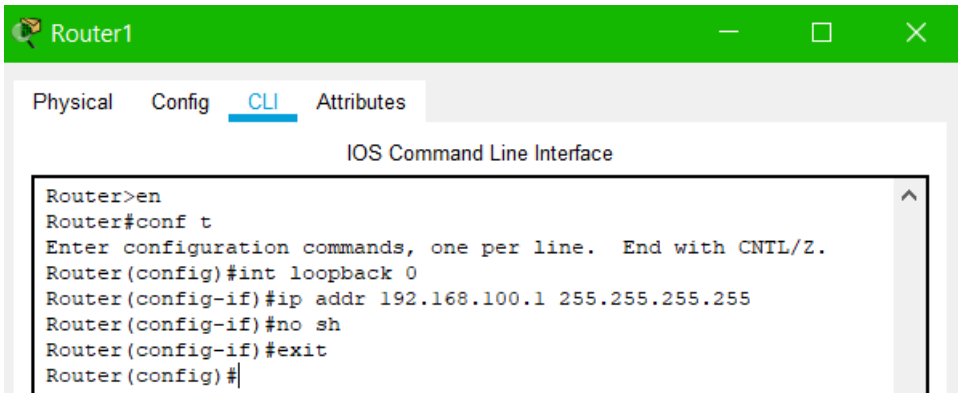


Рис. 14.23. Настраиваем интерфейс loopback на R1

Настраиваем протокол OSPF на R1

Включаем OSPF на R1, все маршрутизаторы должны быть в одной зоне **area 0** (рис. 14.24).

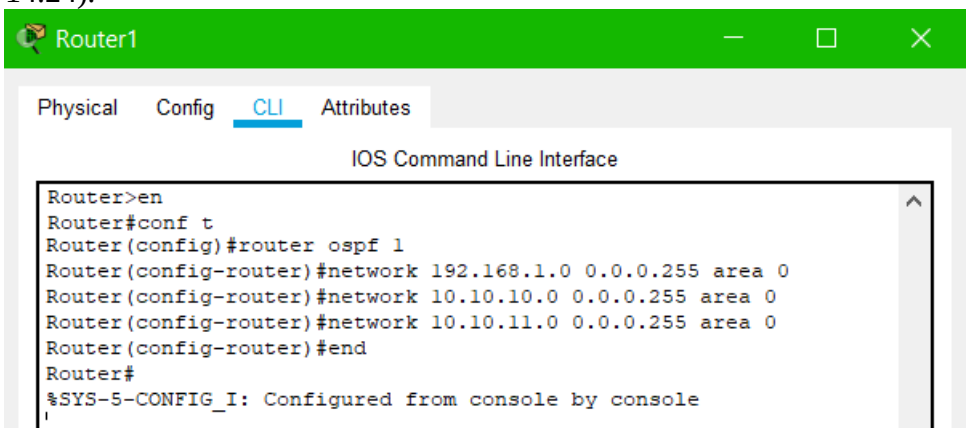


Рис. 14.24. Включаем протокол OSPF на R1

Подводим курсор мыши к R1 и наблюдаем результат наших настроек (рис. 14.25).

```
Port                 Link   VLAN   IP Address         IPv6 Address
GigabitEthernet0/0   Up     --     10.10.10.1/24      <not set>
GigabitEthernet0/1   Up     --     10.10.11.1/24      <not set>
GigabitEthernet0/2   Up     --     192.168.1.1/24     <not set>
Loopback0            Up     --     192.168.100.1/32   <not set>
Vlan1                Down   1      <not set>          <not set>
Hostname: Router
```

Рис. 14.25. Маршрутизатор R1 настроен

Примечание
Обратите внимание, что физически порта 192.168.100.1 нет, он существует только логически (программно).

Настроим loopback интерфейс на R2

На R2 настроим программный loopback интерфейс по аналогии с R1 (рис. 14.26).

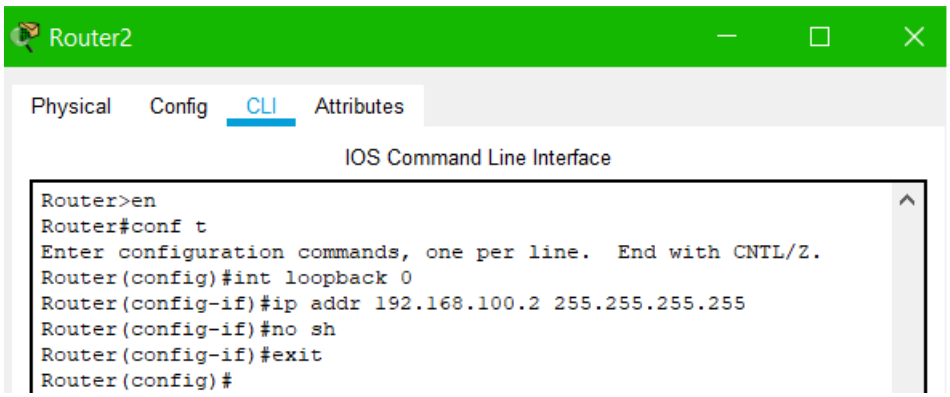


Рис. 14.26. Настраиваем логический интерфейс loopback на R2

Настраиваем OSPF на R2

Включаем протокол OSPF на R2, все маршрутизаторы должны быть в одной зоне area 0 (рис. 14.27).

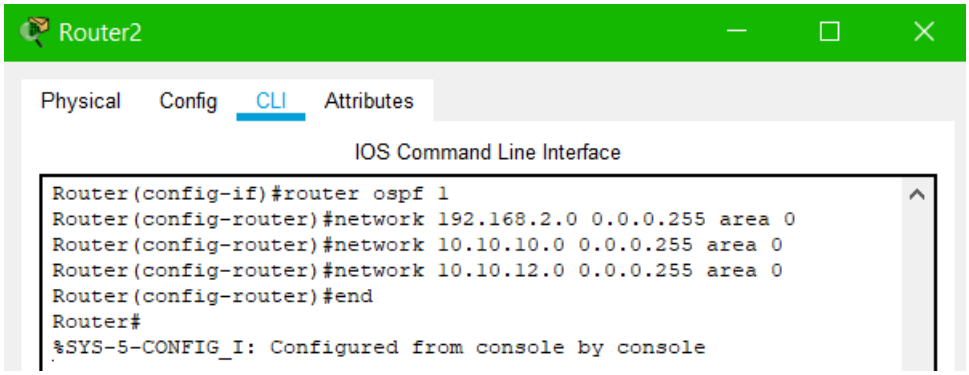


Рис. 14.27. Включаем протокол OSPF на R2

Подводим курсор мыши к R2 и наблюдаем результат наших настроек (рис. 14.28).

```
Port                 Link   VLAN   IP Address          IPv6 Address
GigabitEthernet0/0   Up     --     10.10.10.2/24       <not set>
GigabitEthernet0/1   Up     --     10.10.12.1/24       <not set>
GigabitEthernet0/2   Up     --     192.168.2.1/24      <not set>
Loopback0            Up     --     192.168.100.2/32    <not set>
Vlan1                Down   1      <not set>           <not set>
Hostname: Router
```

Рис. 14.28. Маршрутизатор R2 настроен

Настраиваем loopback интерфейс на R3

Делаем все аналогично (рис. 14.29).

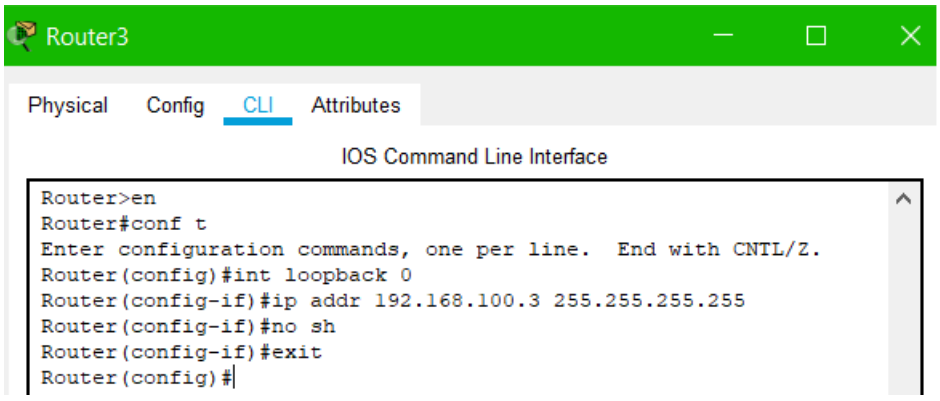


Рис. 14.29. Настраиваем логический интерфейс loopback на R3

Настраиваем протокол OSPF на R3
Здесь делаем все, как раньше (рис. 14.30).

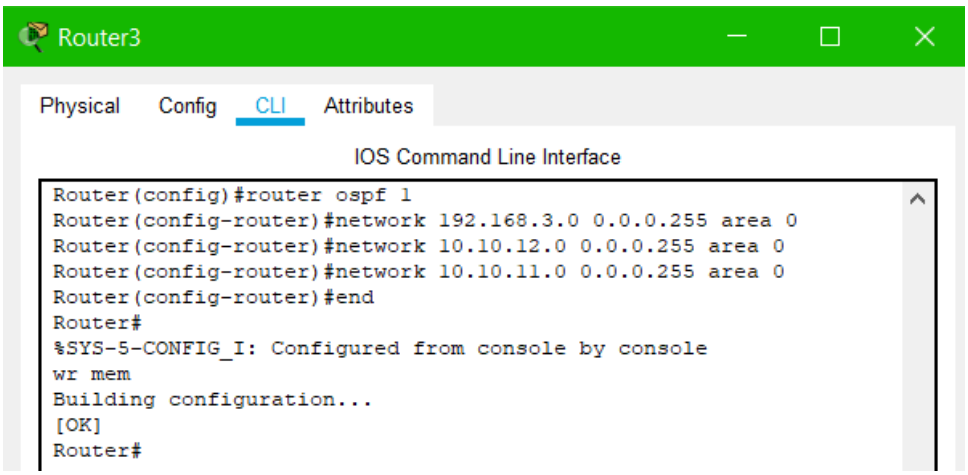


Рис. 14.30. Включаем протокол OSPF на R2

Проверяем результат (рис. 14.31).

```
Port                 Link   VLAN   IP Address
GigabitEthernet0/0   Up     --     10.10.12.2/24
GigabitEthernet0/1   Up     --     192.168.3.1/24
GigabitEthernet0/2   Up     --     10.10.11.2/24
Loopback0            Up     --     192.168.100.3/32
Vlan1                Down   1      <not set>
Hostname: Router
```

Рис. 14.31. Маршрутизатор R3 настроен

Проверяем работу сети

Убеждаемся, что роутер R3 видит R2 и R1 (рис. 14.32.).

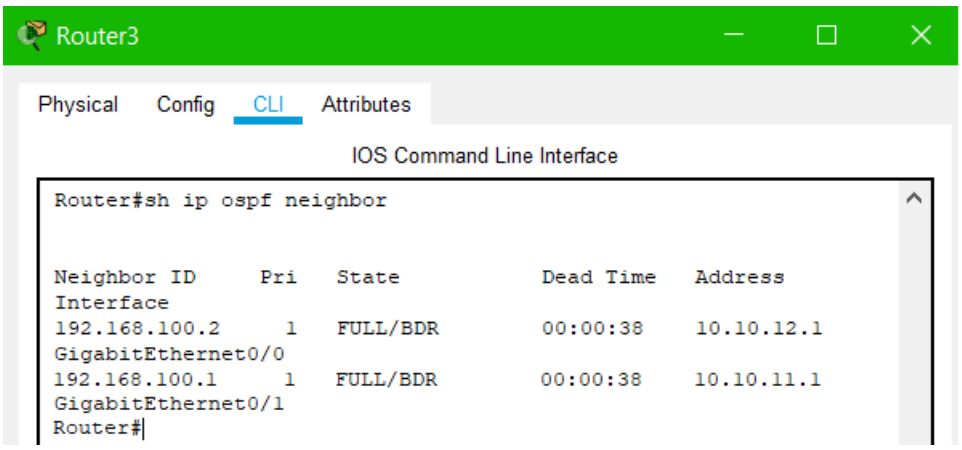


Рис. 14.32 Роутер R3 видит своих соседей

Теперь посмотрим таблицу маршрутизации для R3 (рис. 14.33).

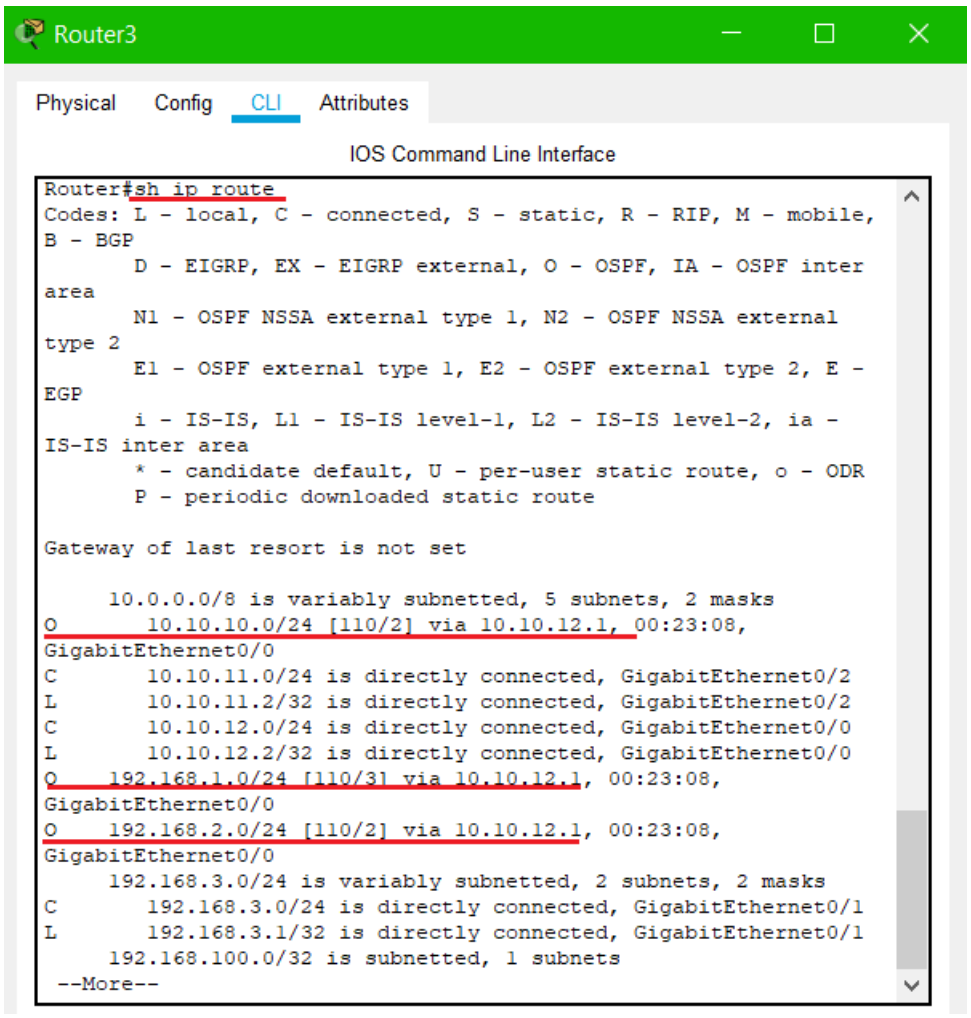
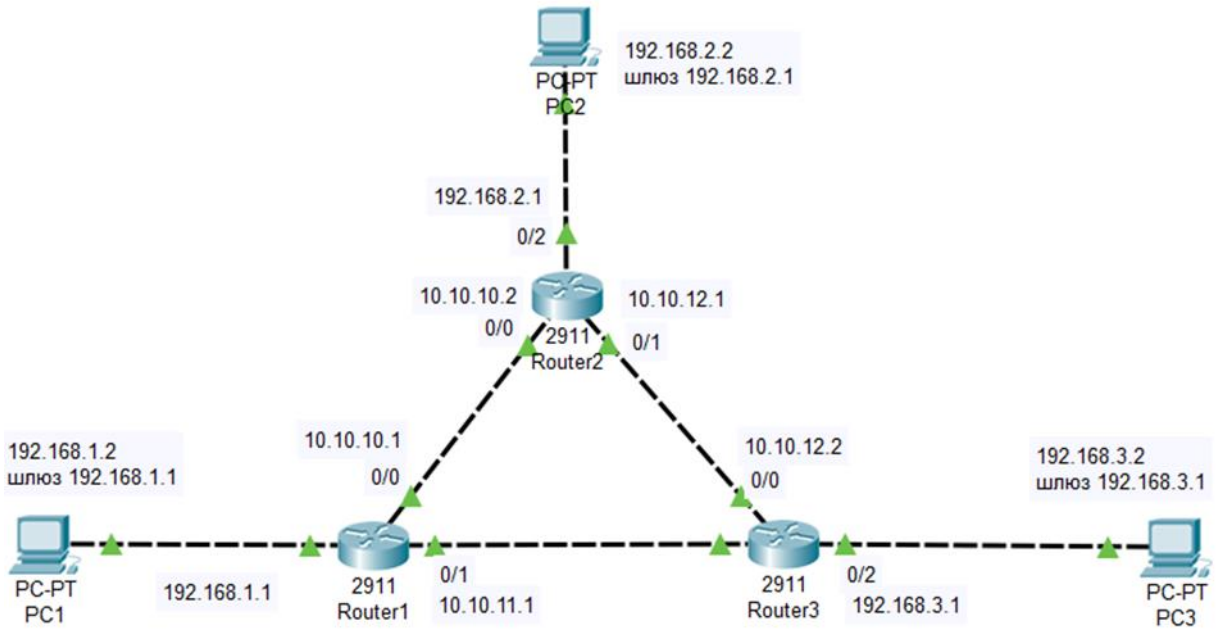


Рис. 14.33. Таблица маршрутизации для R3



Примечание

В этой таблице запись с буквой "O" говорит о том, что данный маршрут прописан протоколом OSPF. Мы видим, что сеть 192.168.1.0 доступна для R3 через адрес 10.10.11.1 (это порт gig0/1 маршрутизатора R1). Аналогично, сеть 192.168.2.0 доступна для R3 через

адрес 10.10.12.1 (это порт gig0/1 маршрутизатора R2). Теперь проверяем доступность разных сетей (рис. 14.34).

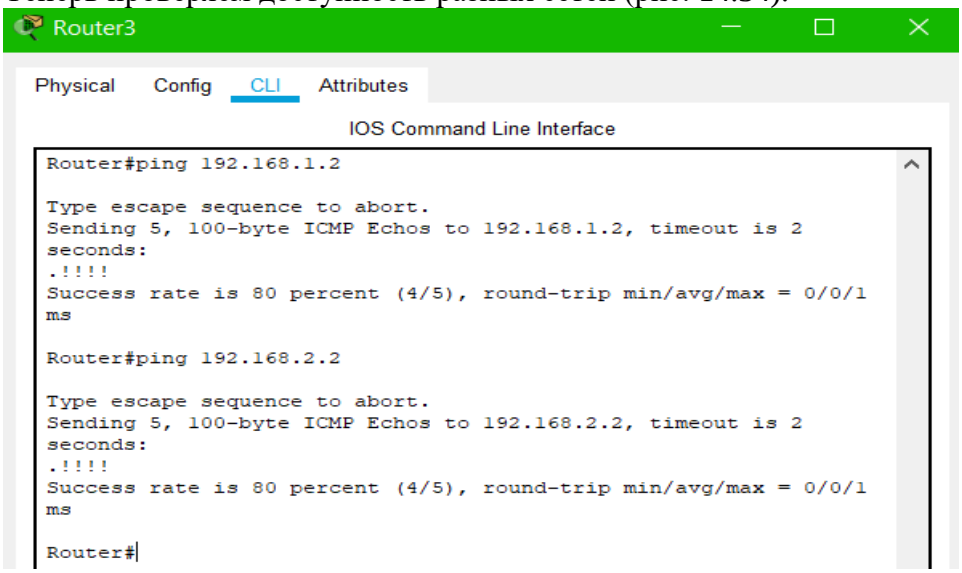


Рис. 14.34. Сети 192.168.1.0 и 192.168.2.0 доступны

15 Самостоятельная работа

Используется составная сеть, структура которой приведена на рис. 1. Все устройства в сети должны иметь параметры Display name и Host name, соответствующие фамилии+имени выполнившего работу студента.

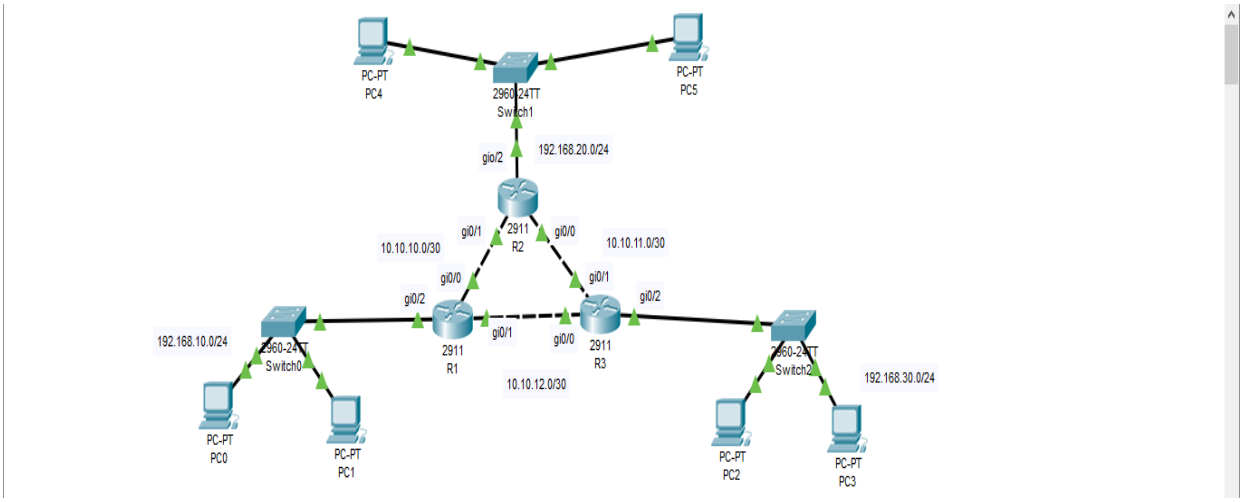


Рис.1. *Составная сеть*

1. Статическая маршрутизация

1. Каждый ПК в составной сети получает IP- адрес по DHCP. DHCP-сервер настроен на маршрутизаторе (R1). Предусмотреть резервирование адресов.
2. Настройте на маршрутизаторах статическую маршрутизацию. На каждом маршрутизаторе посмотрите таблицу маршрутизации. Статических записей должно быть такое же количество, как и при динамической маршрутизации. Сохраните конфигурацию.
3. Показать результаты раздачи адресов сервером в разных сетях.
4. На каждом компьютере выполните команду трассировки других компьютеров.
5. Сохраните проект. Подготовьте отчет, зафиксировав в нем производимые вами действия.

2. Динамическая маршрутизация

1. Каждый ПК получает IP-адрес по DHCP. DHCP-сервер настроен на отдельном сервере (в сети 192.168.10.0). Предусмотреть резервирование адресов.

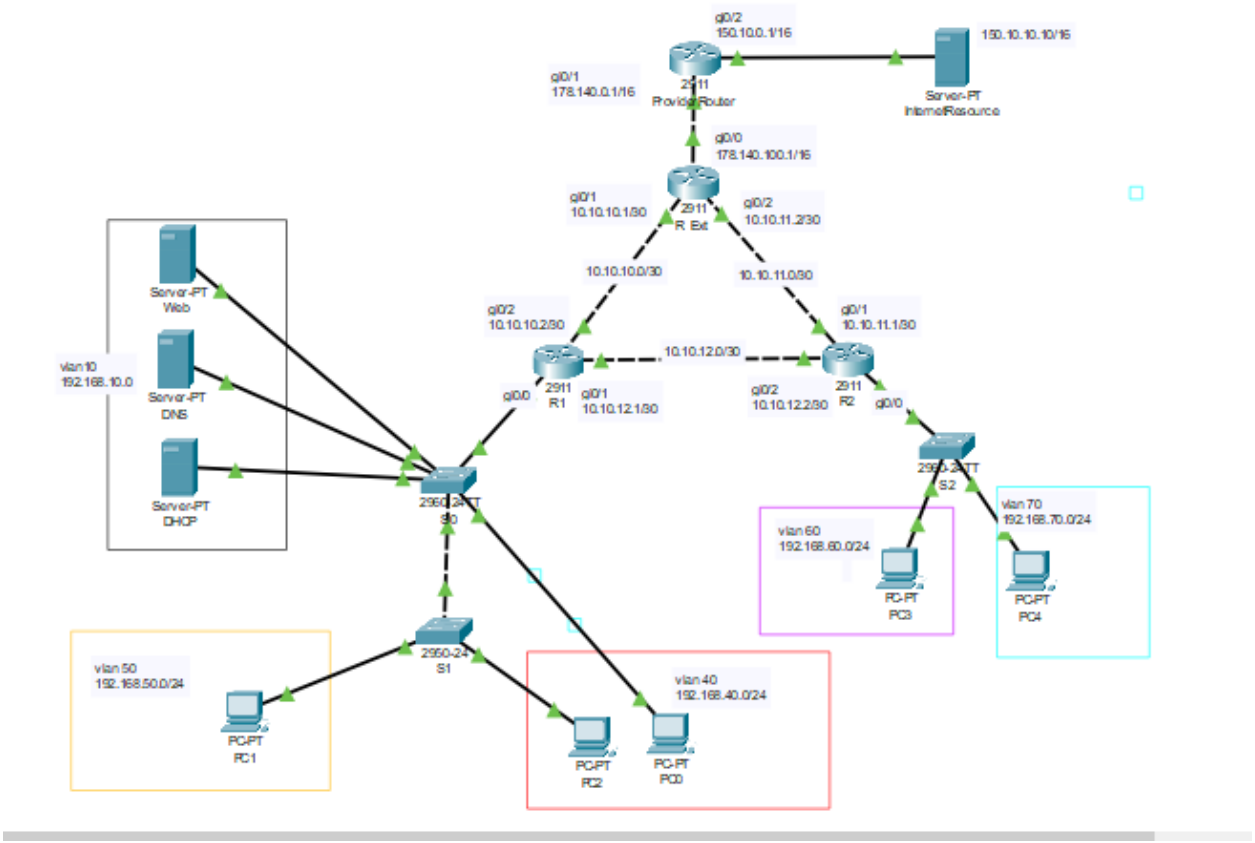
Настройка RIP на маршрутизаторах.

2. Настройте на маршрутизаторах RIP маршрутизацию. На каждом маршрутизаторе посмотрите таблицу маршрутизации. Сохраните конфигурацию.
3. Показать результаты раздачи адресов сервером в разных сетях.
4. С помощью команд *ping* и трассировки проверьте доступность других маршрутизаторов и сетей.
5. Отключите интерфейс между роутерами R1 и R3. Проверьте связь ПК в сетях 192.168.30.0 и 192.168.10.0 с помощью *ping* с количеством пакетов=100. Восстановилась ли связь? Какое количество пакетов потеряно? Посмотрите как изменилась таблица маршрутизации.
6. Сохраните проект. Подготовьте отчет, зафиксировав в нем производимые вами действия.
7. Командой *no router rip* отключите RIP на всех маршрутизаторах, сохраните конфигурацию.

Настройка OSPF на маршрутизаторах.

1. Включите OSPF на всех маршрутизаторах, присвоив процессу номер 10 с областью действия номер 0.
2. Посмотрите изменение в конфигурации каждого маршрутизатора.
3. Показать результаты раздачи адресов сервером в разных сетях.
4. С помощью команд ping и трассировки проверьте доступность других маршрутизаторов.
5. Отключите интерфейс между роутерами R1 и R3. Проверьте связь ПК в сетях 192.168.30.0 и 192.168.10.0 с помощью ping с количеством пакетов=100. Восстановилась ли связь? Какое количество пакетов потеряно? Посмотрите как изменилась таблица маршрутизации.
6. Сохраните проект. Подготовьте отчет, зафиксировав в нем производимые вами действия.

3. Итоговая работа



Задание для итоговой работы:

1. Реализовать сеть, разделенную на 5 vlan: 10, 40, 50, 60 и 70.
2. Настроить VTP на Switch0, Switch1.
3. VLan 10 должна быть доступна из любой другой vlan, в ней находятся все серверы.
4. Конечные узлы других vlan не должны иметь возможности взаимодействовать между собой.
5. Во vlan 10 реализовать:

• Web сервер. Создайте на нем страницу index.html с текстом «I (your name) AM SUPER»:

• DNS сервер содержит доменную запись «super.ru», указывающую на Web сервер.

• DHCP сервер содержит пулы адресов для отдельной подсети каждой vlan.

6. DHCP раздает адреса во все подсети (в каждую vlan). Из каждого пула адресов (определенной VLAN) исключить первые пять адресов.

На роутере настроить соответствующие списки доступа.

7. Для всех подинтерфейсов, кроме предназначенного для vlan 10, настроить 192.168.10.2 как DHCP relay (использовать команду helper address). По данному адресу будет располагаться DHCP сервер, поэтому широковещательные DHCP запросы из подсетей транслируются на DHCP сервер.
8. Для DHCP сервера использовать доверенный порт.
9. Реализовать во внутренней сети динамическую маршрутизацию по протоколу OSPF.
10. Пограничный маршрутизатор предоставляет доступ внутренней сети к внешней, разделяя их динамическим NAT.

11. Все устройства в сети должны иметь параметры Display name и Host name, соответствующие фамилии+имени выполнившего работу студента.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем заключается задача маршрутизации?
2. Что такое маршрутизатор?
3. Перечислите основные компоненты маршрута.
4. Что такое административное расстояние? Перечислите его значения для нескольких видов маршрутизации.
5. Что такое петля маршрутизации? Как с ней бороться?
6. Что такое статическая маршрутизация? Что в ней обозначается буквами C и
7. S?
8. В каких случаях применяется статическая маршрутизация?
9. Приведите команды для конфигурации интерфейсов маршрутизатора Cisco.
10. Какими командами можно просмотреть конфигурацию интерфейсов маршрутизатора?
11. Для чего необходим маршрут по умолчанию, как его установить?
12. Как проверить работоспобность сети?
13. Как называется технология, предотвращающая передачу информации о маршруте обратно маршрутизатору, от которого получил данную информацию?
14. Какой порт и протокол транспортного уровня используются при распространении обновлений RIP?
15. Чему равен период рассылки обновлений в RIP?
16. Когда сеть-получатель по RIP считается недостижимой?
17. К какому классу алгоритмов относится протокол маршрутной информации?
18. Чему равен период рассылки обновлений в OSPF?
19. К какому классу алгоритмов относится протокол OSPF?
20. С помощью какой команды выводится список соседей маршрутизатора?